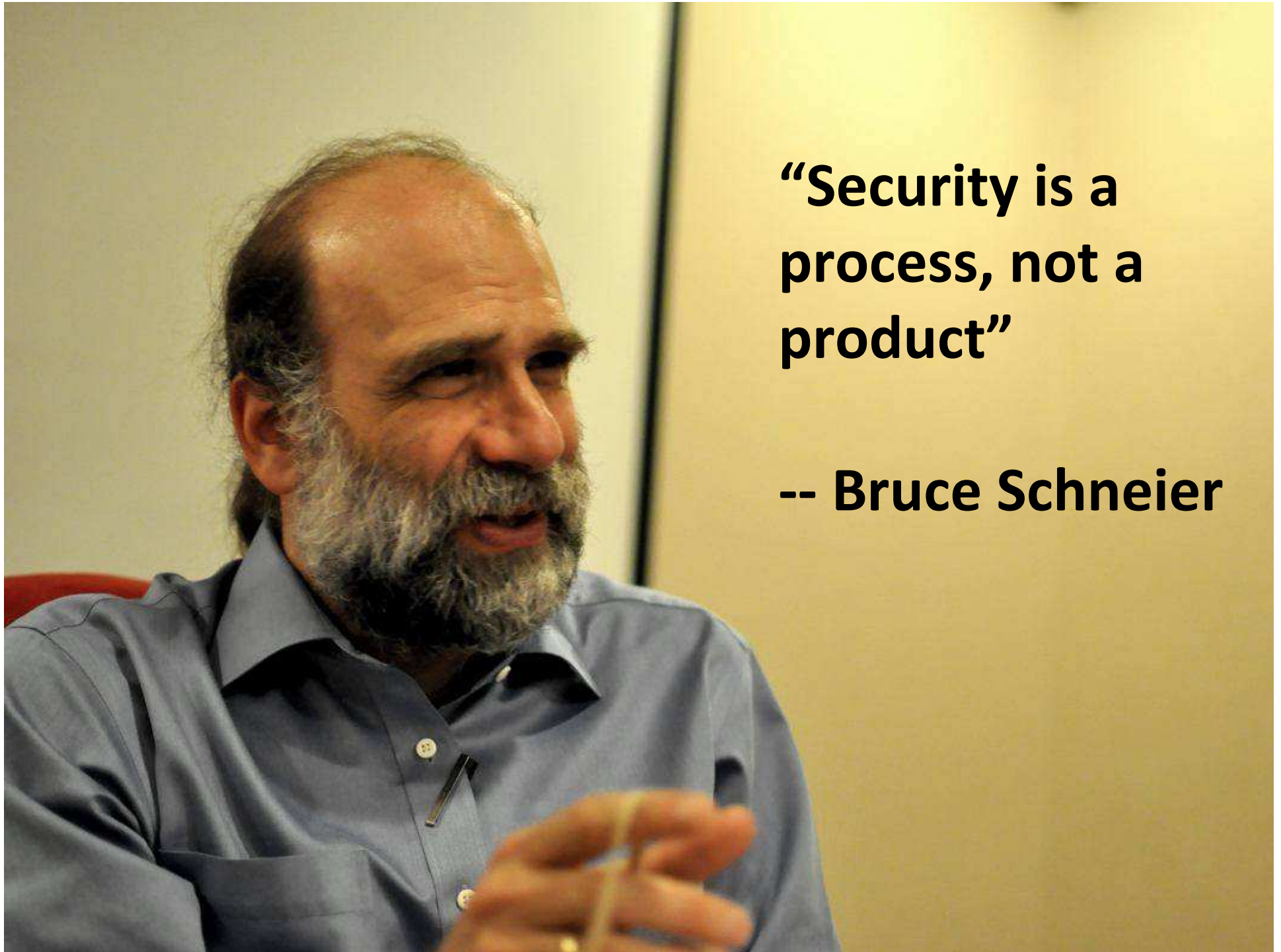




THE OPEN WEB APPLICATION SECURITY PROJECT





**“Security is a
process, not a
product”**

-- Bruce Schneier

What if the
software world
was only...



100 apps written by 100 developers at 100 companies

A close-up photograph of a small, spotted fawn being gently held by a person's hand. The fawn has a brown body with white spots and a dark stripe running down its back. It has large, dark eyes and small ears. The person's hand, which is wearing a ring with a dark stone, is visible in the foreground, supporting the fawn. The background is a plain, light-colored surface.

83

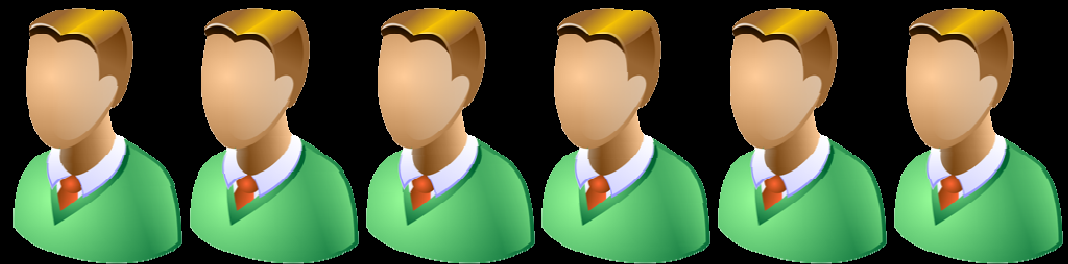
apps have a serious vulnerability

72




apps have Cross Site Scripting

40



apps have SQL injection



1

company has a
responsible appsec program

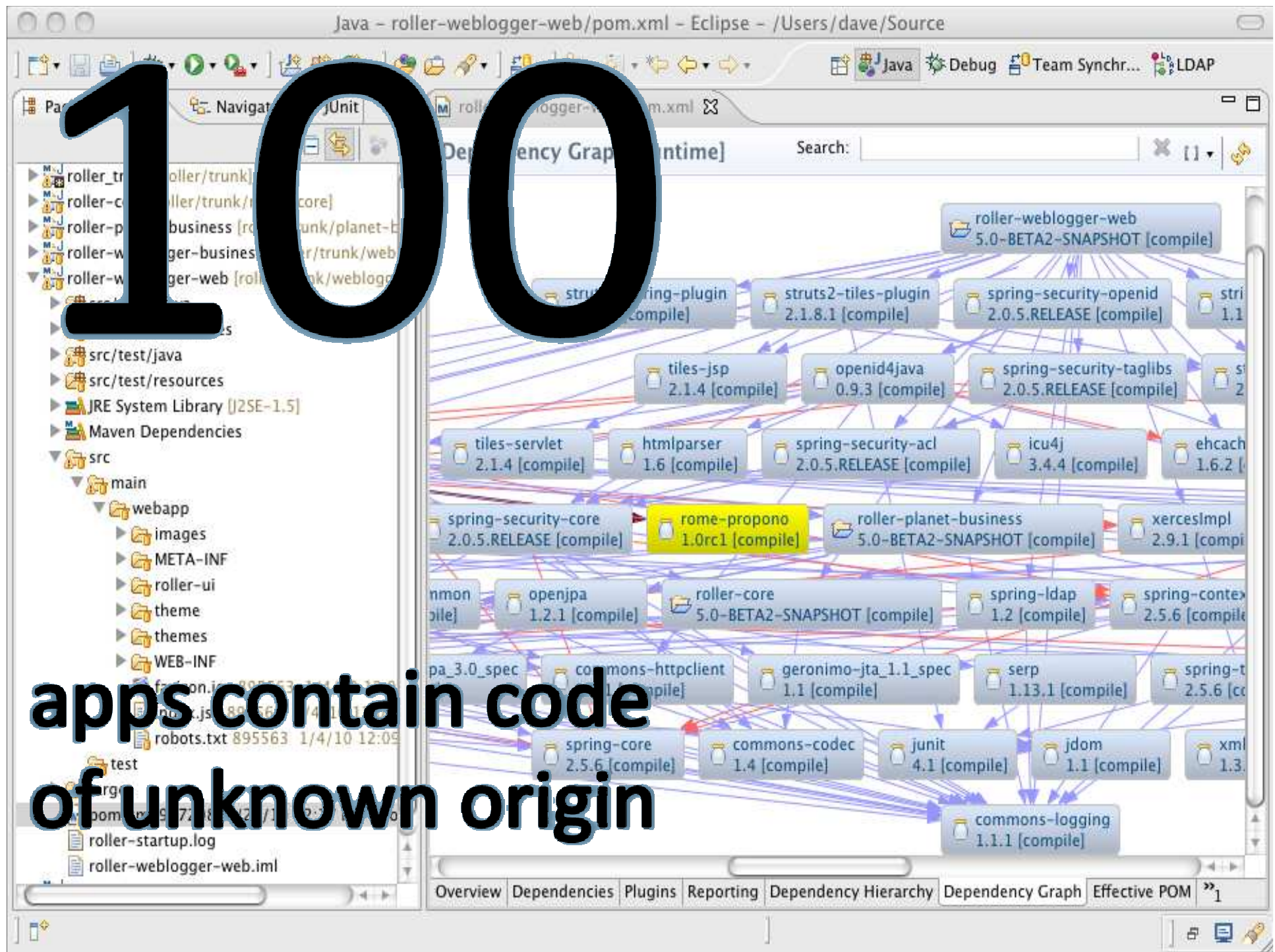
A large group of people, mostly men, are posed in many rows for a group photo at what appears to be a conference or meeting. They are dressed in business casual attire. A red circle with a white border highlights a woman in the middle of the group. A large, stylized number '1' is in the top right corner.

1

developer has any security training

100

apps contain code
of unknown origin



90



apps use unpatched libraries
with known flaws

TB TOTAL BODY

5

ANTERIOR

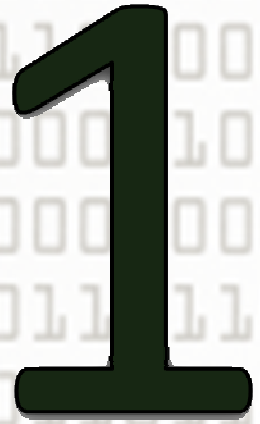
ANTERIOR

POSTERIOR

POSTERIOR


18.73 MCI 99MTC HDP
(RAC IV)

apps have had a scan or pentest



1

**app has had a manual
security code review**





0

**apps provide any
visibility into security**

Why?



“Don’t hate the playa

Hate the game”

-- Ice T



The first rule of security is...



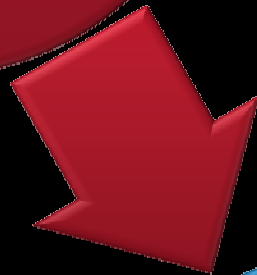
...You do not talk about security

Toxic?

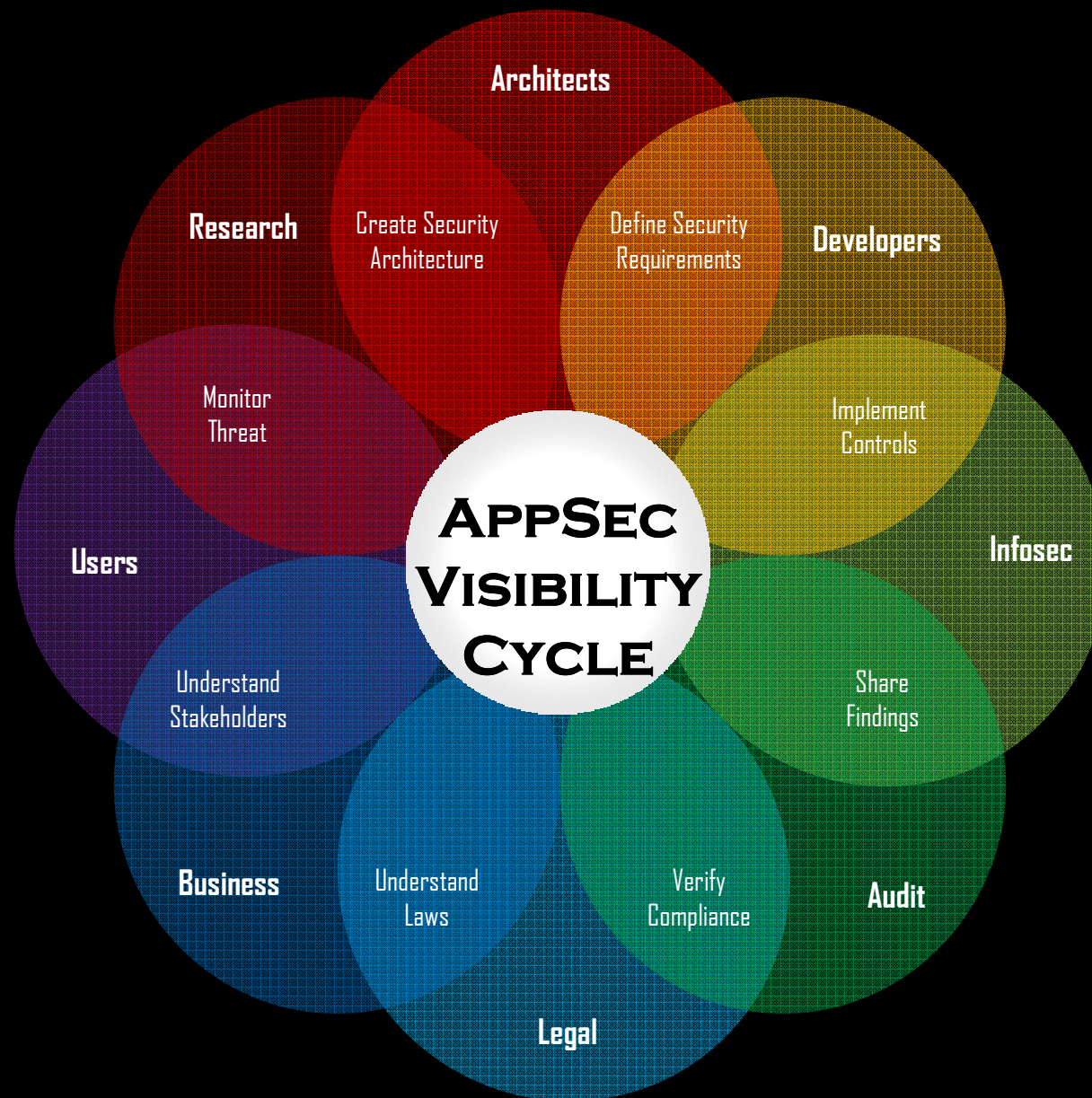
We
Trust

We
Hide

We
Blame



Our Mission: Visibility



Security Facts

Type: Web Application

Jun 28, 2010

OWASP Top 10 2010

A1-Injection	<input type="radio"/>
A2-Cross Site Scripting (XSS)	<input checked="" type="radio"/>
A3-Authentication	<input checked="" type="radio"/>
A4-Object References	<input type="radio"/>
A5-Cross Site Request Forgery	<input type="radio"/>
A6-Security Configuration	<input type="radio"/>
A7-Cryptographic Storage	<input checked="" type="radio"/>
A8-URL Access Control	<input type="radio"/>
A9-Transport Layer Protection	<input checked="" type="radio"/>
A10-Redirects and Forwards	<input type="radio"/>

Custom Code

Name	Language	LOC
Core	Java	1200K
Developer Plugin	Java	20K
Reporting Plugin	Java	12K
Persistence Layer	PSQL	15K
User Interface	JSF	46K
Business Functions	Java	102K

Libraries

Name	Language	H	U
Struts 1.1	Java	<input type="radio"/>	<input checked="" type="radio"/>
Log4j 1.0.3	Java	<input type="radio"/>	<input type="radio"/>
XOM 2.1	Java	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Hibernate 3.0	Java	<input checked="" type="radio"/>	<input type="radio"/>
OWASP ESAPI 2.0rc6	Java	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Platform Components

Name	Language	H	U
WebSphere 6.1.2	C/C++	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Java Enterprise Edition 3.1	Java	<input checked="" type="radio"/>	<input type="radio"/>

Interfaces and Connections

Name	Protocol	D	E	N	Z
Web Interface	HTTPS	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
FTP Interface	FTP	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Google Search API	REST	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sybase	TDS	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Oracle 11	SOAP	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Log Server	SNMP	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Mainframe	SNA	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Sensitive Data

Name	Concerns	S	T	Z
Healthcare Records	CIA	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Credit Card Numbers	CI	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Growing Ecosystems

Home - PythonSecu... x

← → ↻ 🏠 ☆ http://www.pythonsecurity.org/

Python Security topics software google group

Home

Welcome to Python Security, the home of the largest collection of information about security in the [Python](#) programming language.

Our mission is to make Python **the most secure programming language in the world**, ensure hackers **never** break a Python-based application, and make security breaches **a thing of the past!**

This site contains a vast amount of security information, organized into two sections:

- Security topics and how they relate to Python as a whole
- The security of specific software such as frameworks and template engines

We also have a [Google Group](#), on which you may ask or discuss anything related to security in Python.

We Need YOUR Help

PythonSecurity.org is a blossoming community, and we need your help to make it grow. Here are a few ways in which you could help:

- Contribute to the currently focused article: [Session Management](#)
- [Submit](#) a relevant link or piece of news
- Contribute fixes and patches to software projects to improve security
- Spread the word!

Security Topics

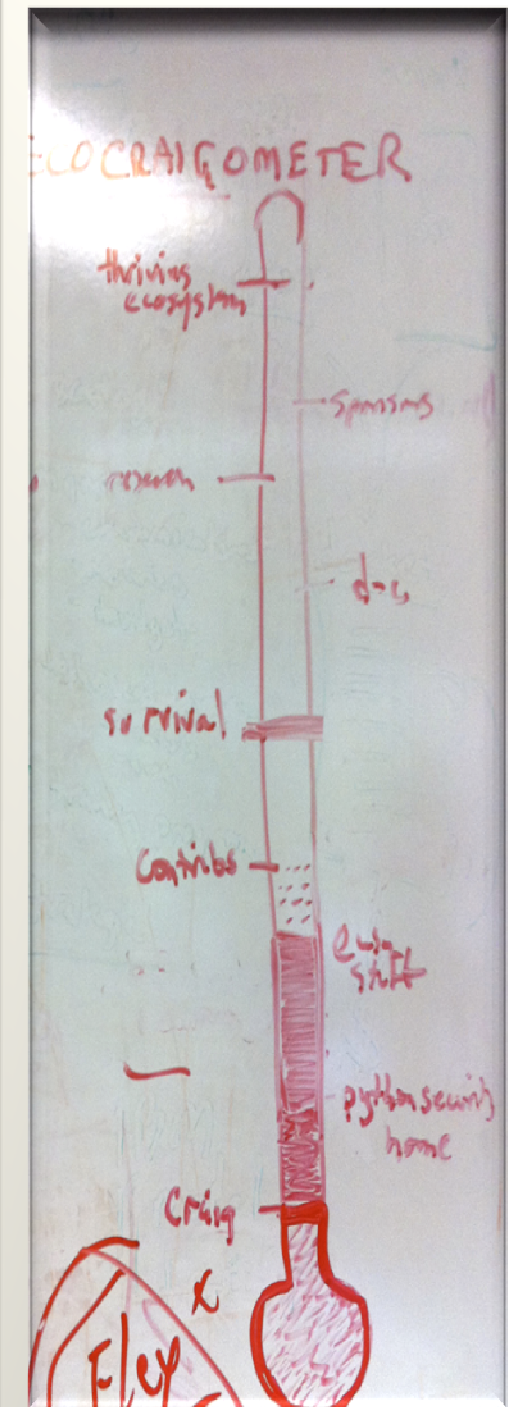
- [Access Control/Authorization](#)
- [Authentication](#)

Software

- [Web Frameworks](#)
- [Bottle](#)

Cheat Sheets

- [Template Engines](#)
- [Chameleon](#)



OWASP Meritocracy

OWASP Users and Participants



OWASP Members

OWASP Leaders
(Chapters and Project)

Projects

Membership

Education

Conferences

Industry

Chapters

Connections

OWASP Foundation
(OWASP Board)



Today

- Getting Started with OWASP T10 and Guides
- Building a Software Assurance Program
- Using the OWASP Live CD

====LUNCH====

- OWASP Enterprise Security API (ESAPI)
- OWASP O2
- The DISA AppSec STIG and OWASP Tools
- Discussion

Jeff Williams
Aspect Security CEO
OWASP Foundation Chair
jeff.williams@owasp.org
<http://www.owasp.org>
twitter @planetlevel
410-707-1487

Join Us

